1. Approval and Authorisation

Completion of the following signature blocks signifies the review and approval of this Process (signed copy held in safe)

Name	Job Title	Signature	Date
Authored by:- <Name>	Director of Finance & IT		
Approved by:- <Name>	Information Security Officer		
Authorised by:- <Name>	Director of Finance & IT		

2. Change History

Version	Date	Reason
Draft 1.0		First draft for comments
Version 1.0		First Version
Version 1.1		<Reason>

3. Contents

4. Definitions in this report

Trust	XXXXX NHS Trust
MS NT	Microsoft Windows NT operating system
ISO	Information Security Officer
Helpdesk, National	IT Helpdesk email

5. Documents referred

ISMS/REV/001	Review of Privileges

6. Introduction

The purpose of this policy is to prevent unauthorised access to the Trust's information systems. The policy describes the registration and de-registration process for all TRUST information systems and services.

These policies apply especially to new starters, leavers and those moving job, responsibility or Portfolio.

These policies should also be seen in the light of HR procedures to verify a new starters qualifications, references and right to work in this country.

7. User registration

7.1 New Users

Access to Trust information services is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.

Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out (ie. Training).

There is a standard level of access (xxx, xxxxx, document scanning, xxxx and the xxxxxxxx database), other services can be accessed when specifically authorised by HR/line management.

A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR. The request is free format, but must state:

- Name of person making request
- Job title of the newcomers and workgroup
- Start date
- Services required (default services are: MS Outlook, MS Office and Internet access)

Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure.

The user signs the form indicating that they understand the conditions of access.

Access to all TRUST systems is provided by IT and can only be started after proper procedures are completed .

A new user will be set up on receipt of written notification but not made available, by issue of password, until the individual's start date.

IT will maintain a record of all requests in a folder named "new users" in the Helpdesk, National mailbox and will file email paper copies in the user access file.

7.2 Change of user requirements

Changed requirements will normally relate to an alteration to the applications used but may also involve network access. Requests must be in writing (e-mail or hard copy) and must be directed to the Helpdesk.

Changes will be made on receipt of a properly completed request, the same details as shown above are required and requests will be filed under “access change requests” in the Helpdesk, National mailbox.

The ISO will not normally be copied in on requests but must be consulted if the request is not for a standard network service.

7.3 Change of password

Where a user has forgotten his/her password, the helpdesk is authorised to issue a replacement.

Upon receipt of such a request the Helpdesk will

1. Ensure the request is logged.
2. Confirm the identity of the user by question about existing services/access or by reference to a work colleague
3. Issue a temporary, single use, password which will require the user to set up a formal password.

7.4 Removal of users

As soon as an individual leaves the Trust’s employment, all his/her system logons must be revoked.

As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

All notification will be filed in a folder called “Leavers” in the Helpdesk, National mailbox.

Additionally, IT operations will positively confirm leavers with HR, each Friday, retaining a copy of the e-mail and reply in a file “Leavers” in the Helpdesk, National mailbox, or hard copy in the user access file.

Unless otherwise advised, IT operations will delete network access for all leavers at 4pm each Friday (or on the leaving date if not a Friday) (old user ID's are removed and not re-issued). This will include access to all network services. IT operations will inform application owners of leavers where their systems are affected.

The Trust expects all leavers to hand over current files within their workgroup, however IT operations can move a leavers files to specific areas if requested. Normally a leaver's data will be left in its existing directory for one month and then archived off system (but can be recovered if required).

8. Privilege management

(Please also refer to the Review of Privileges procedure).

"Special privileges" are those allowed to the system manager or systems programmers, allowing access to sensitive area (for example, passwords). The unnecessary allocation and use of special privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached

Privileged access must be authorised by the Director of xxxxxxxxxxxx, using the request form shown in Appendix 1. All completed forms, both current and expired, will be held by the ISO who is authorised by the completed form to set up the access specified.

All requests for access outside normal services must be supported by a completed and authorised Privilege Access form.

The Director of xxxxxxxxxxxx will maintain a master list of privileged accesses, which are in use, and this will be checked and confirmed by the ISO on a three monthly basis. The list will identify all separate logons for each system and service.

9. User password management

Password format and general rules are held within the Information Security – A Guide to Staff. Systems logon requires that all passwords be of a minimum of 7 characters.

Temporary access may be granted on a need to use basis. Such logons may be granted by the ISO (in the Director of xxxxxxxxxxxxxx absence) but must be recorded and reported on the normal form. Temporary logons must be identified by a specific login (starting TEMP****) and must be deleted immediately after use.

10. Review of user access rights

The ISO will institute a review of all network access rights at least twice a year, which is designed to positively confirm all users.

Any lapsed or unwanted logons, which are identified, will be disabled immediately and will be deleted unless positively reconfirmed.

Annually, the ISO will institute a review of access to applications. This will be done in cooperation with the application owner and will be designed to positively re-confirm all users. All other logons will be deleted.

The review will be conducted as follows.

- The ISO will generate a list of users, by application.
- The appropriate list will be sent to each Application owner who will be asked to confirm that all users identified are authorised to use the system.
- The ISO will ensure a response.
- Any user not confirmed will have his/her access to the system removed.
- The ISO will maintain a file of -
    - Lists sent over
    - Application owner responses
    - A record of action taken
- The review will normally be conducted in <Month> and <Month>

Appendix 1 – Request for Privileged Access

Name of applicant: _____

Job Title: _____

Permanent
Temporary

Delete as appropriate

Access requested for:

Systems	Login Name	Access Level	Reason

Access required: **From date:** _____

To date: _____

Applicant signature: _____

System owner name: _____

System owner's comments: _____

_____

System owner's authorisation: _____

Approved by:
Director of xxxxxxxxxxx _____